DSB Task Force on

CYBER SUPPLY CHAIN

THIS PAGE INTENTIONALLY BLANK

REPORT OF THE DEFENSE SCIENCE BOARD

TASK FORCE ON

Cyber Supply Chain

April 2017

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense. The Defense Science Board Task Force on Cyber Supply Chain completed its information-gathering in May 2016. The Executive Summary was cleared for public release on April 17, 2017.

The Executive Summary is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISITICS

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber Supply Chain

I am pleased to forward the final report of the DSB Task Force on Cyber Supply Chain. The study proposes recommendations to strengthen the supply chain of microelectronics that are inserted into Department of Defense weapons systems.

Given the dynamic nature of the global market for microelectronics, the Department must operate in a rapidly evolving environment to assure parts in the cyber supply chain. The report recommends expanding cyber supply chain exercises in the Military Services to address warfighter challenges while also improving program protection practices over the lifecycle of weapons systems.

I fully endorse all of the recommendations contained in this report and urge their careful consideration and adoption.

Craig Fields
Chairman

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Task Force on Cyber Supply Chain

Attached is the final report of the Defense Science Board Task Force on Cyber Supply Chain. The task force assessed the organization, missions, and authorities that encompass the use of microelectronics and components in Department of Defense (DoD) weapons systems. The task force addressed:

- practices to mitigate malicious supply chain risk and latent vulnerabilities, and whether opportunities exist to modify or strengthen these practices;
- current Department program protection processes, as well as other practices to detect and assess potential vulnerabilities in hardware and software;
- the extent to which commercial off the shelf vulnerabilities have been reported and impact the security of DoD systems; and
- interagency activities that DoD could better leverage to reduce supply chain risks.

The task force found that the capital cost of maintaining a DoD-owned Trusted Foundry is not a feasible expense. The task force recommends that the Department develop a long-term strategy for access to state-of-the-art commercial foundry capabilities that does not rely exclusively on trust; and continue research and development (R&D) investments of DoD agencies for a technology-enabled strategy that fosters new tools to better defend against cyber supply chain attacks.

The task force concluded that the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) must strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that DoD weapons systems are designed, fielded, and sustained in a way that reduces the likelihood and consequences of cyber supply chain attacks.

Hon. Paul “Page” Hoeper
Co-chair

Dr. John Manferdelli
Co-chair

Table of Contents

Executive Summary

Modern weapons systems have depended on microelectronics since the inception of integrated circuits over fifty years ago. Today, most electronics contain programmable components of ever increasing complexity.[1, 2] At the same time, the Department of Defense (DoD) has become a far less influential buyer in a vast, globalized supplier base.[3] Consequently, assuring that defense electronics are free from vulnerabilities is a daunting task.[4]

Because system configurations typically remain unchanged for very long periods of time, compromising microelectronics can create persistent vulnerabilities. Exploitation of vulnerabilities in microelectronics and embedded software can cause mission failure in modern weapons systems. Such exploitations are especially pernicious because they can be difficult to distinguish from electrical or mechanical failures and because effects can run the gamut from system degradation to system failure to system subversion.

Cyber supply chain vulnerabilities may be inserted or discovered throughout the lifecycle of a system. Of particular concern are the weapons the nation depends upon today; almost all were developed, acquired, and fielded without formal protection plans.

MALICIOUS INSERTION AND THE EXPLOITATION OF LATENT VULNERABILITIES

Insertion of a malicious microelectronic vulnerability via the supply chain can occur at any time during production and fielding of a weapons system or during sustainment of the fielded system. No matter where an attack occurs in the lifecycle of the system, an attacker seeking to exploit a maliciously inserted vulnerability must execute each step in the kill chain:

- **Intelligence and planning:** gathering information on target system and suppliers to develop supply chain attack vector.
- **Design and create:** developing malicious hardware or software for insertion into target supply chain. May be done in an attacker-owned facility or by an insider in a legitimate facility.
- **Insert:** incorporating malicious hardware or software into target system through its supply chain.
- **Achieve effect:** actuating and operating malicious hardware or software to achieve an effect.

1. For example, the BA 5590 battery, used in numerous systems, incorporates a “smart” state-of-charge indicator.
2. Basic input and output system (BIOS) complexity increased by a factor of 10^6 between 1999 and 2015.
3. DoD now buys less than one percent of application specific integrated circuits (ASICs), and an even smaller percentage of commodity electronics.
4. See Appendix A for a discussion of fundamental approaches to assurance.

Executive Summary

While there has been some emphasis on denying the attacker information about the target system and suppliers, DoD has focused primarily on denying malicious insertion through use of "trusted" sources, where trust is determined by the pedigree of the supplier.

The task force observed instances that may have been unsuccessful attacks on critical weapons systems via malicious insertion. It is difficult to know whether such activity is widespread, but the existence of counterfeit electronics in the supply chain demonstrates the potential for such attacks.[5] When done effectively, malicious insertion will not be detectible until actuated and it may present as a design flaw when ultimately observed.

Exploitation via malicious insertion has, however, been confirmed in the commercial sector. Prominent recent examples include Volkswagen's insertion of a "defeat device" to thwart emissions testing and insertion of embedded code into Juniper® routers.[6, 7] Recently, FTDI, a semiconductor device company, used a Windows driver update to completely disable computers using functional clones of some component chips, demonstrating the full cycle of component insertion, subsequent activation, and effect.[8]

Complex microelectronics will inevitably contain latent vulnerabilities. Diligent test protocols, while an essential best practice, cannot guarantee that systems will be free of such vulnerabilities.[9] Vulnerabilities in widely distributed commercial microelectronics have been discovered years after these components were sold into the market.[10] Even where no single major vulnerability exists, attacks may exploit a series of subtle design issues that may be widely distributed.[11] If an attacker can gain access to weapons system design information and discover a useful latent vulnerability, it is possible to bypass the costly and potentially risky process of malicious insertion.

5. Department of Commerce, *Defense Industrial Base Assessment: Counterfeit Electronics*, [January 2010]. Available at: https://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010 (Accessed September 2016.)
6. Russell Hotten, "Volkswagen: The scandal explained." *BBC News* [December 10, 2015]. Available at: www.bbc.com/news/business-34324772 (Accessed October 2016.)
7. Brad Duncan, October 28, 2016 (12:51 p.m.), "ScreenOS vulnerability affects Juniper firewalls," InfoSec Handlers Diary Blog, [December 18, 2015]. Available at: https://isc.sans.edu/diary/ScreenOS+vulnerability+affects+Juniper+firewalls/20511 (Accessed October 2016.)
8. James Sanders, "FTDI abuses Windows Update, pushing driver that breaks counterfeit chips," *TechRepublic* [February 2, 2016]. Available at: http://www.techrepublic.com/article/ftdi-abuses-windows-update-pushing-driver-that-breaks-counterfeit-chips (Accessed September 2016.)
9. This is true for all but the simplest systems.
10. For example, dynamic random-access memory (DRAM) modules susceptible to the Rowhammer effect were produced beginning in 2010. The vulnerability of these DRAMs to attack leading to privilege escalation was published in 2015. Essentially all computers manufactured during this period had this vulnerability. See *Google Project Zero* blog, available at: https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html (Accessed December 2016.)
11. Andy Greenberg, "Wickedly Clever USB Stick Installs a Backdoor on Locked PCs," *Wired Magazine*, [November 16, 2016]. Available at: www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/?mbid=social_gplus (Accessed December 2016.)

The extended lifecycles of defense systems increase the probability that an attacker will both gain system knowledge and also discover latent vulnerabilities. Recent exercises by all three Military Services have demonstrated the feasibility and efficacy of exploitation via this shortcut to achieve the desired effect.

OVERVIEW OF THE CYBER SUPPLY CHAIN LANDSCAPE

The supply chain for microelectronics parts is complex, involving multiple industry sectors. Each sector sells to each of the others. Furthermore, parts may be returned to manufacturers or distributors and subsequently reenter the supply chain making both pedigree and provenance difficult to track using current procedures. This complex of industry segments feeds three supply chains: the DoD acquisition supply chain, the DoD sustainment supply chain, and the global commercial supply chain. Each supply chain is subject to attack and each offers differing costs and benefits to an attacker.

In 2011, recognizing the DoD's heavy reliance on integrated circuits produced outside the United States to achieve cutting edge technology, the Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) instructed program managers (PMs) to address supply chain threats in their Program Protection Plans (PPPs). PPPs are intended to take a comprehensive approach in considering all aspects of system security, including cybersecurity, and address initial steps to safeguard unclassified program information.

Programs subject to milestone decisions are required to conduct program protection activities and document the results in PPPs for approval by the Milestone Decision Authority at each acquisition milestone. Review of the program protection processes across the Department shows that security and information system managers address security primarily after the system design has been completed.

Current PPPs, however, do not carry over robustly to the sustainment phase. There is little evidence that robust program protection activities continue after a system has been fielded or that documentation is being maintained as the system continues to evolve through sustainment. By the time a defense system is fielded, microelectronic components in that system are likely to be obsolete and may be unavailable from the original equipment manufacturer (OEM) or its sub-tier suppliers. This may force DoD to purchase from distributors where pedigree is less secure and provenance is more difficult to track. Furthermore, the longer a system is in the field with the same microelectronic parts and embedded software, the more likely it is that adversaries will be able to gain system information and to insert or discover vulnerabilities. As these vulnerabilities have been revealed, it has become clear that malicious insertion and discovery of exploitable latent vulnerabilities are concerns in both the acquisition and sustainment supply chains.

Active search and automated monitoring can expose vulnerabilities. Cyber Awakening exercises have discovered exploitable cyber supply chain vulnerabilities in key weapons systems. The results of such exercises, if conducted regularly on major weapons systems and subsystems, would be highly relevant for systems currently in both acquisition and sustainment. There is not yet a mechanism for routinely providing cyber awareness results to Program Executive Offices (PEOs) and program

managers, or cyber awareness training to logisticians and hands-on maintenance personnel at appropriate classification levels.

Program management offices are responsible for creating Program Protection Plans. Currently, guidance, expertise, and support for this effort are insufficient, with limited engagement by the system engineering community and limited influence on system design. Program protection planning activities are uneven in quality and focus as some programs focus on protecting microelectronics availability whereas others emphasize protection of personnel or system security. The task force believes that the proper focus should be on reducing the probability of mission failure. The Joint Federated Assurance Center (JFAC) should be used as a much needed source of expertise in support of program managers to assist with life cycle program protection planning and system security engineering.

In typically long DoD acquisition processes, approximately 70 percent of electronics in a weapons system are obsolete or no longer in production prior to system fielding.[12] The Department's mechanisms for tracking inventory obsolescence and vulnerabilities in microelectronic parts are inadequate. Microelectronics components are likely to become obsolete repeatedly during the weapons system lifecycle. Efforts to track component obsolescence lack oversight at a Department-wide level.[13] Reporting of counterfeit and "suspect-counterfeit" microelectronics is mandatory for some, but not all prime contracts and subcontracts. Such reporting requirements are inconsistent and no DoD system at present collects event information on cyber-physical attacks of electronic components as its primary function. To address these concerns, a shared vulnerability database and a parts application database of installed hardware could promulgate corrective actions across weapons systems.

DoD will have a continuing need for access to trustworthy, state-of-the-art, application specific integrated circuits (ASICs). That need is likely to grow for systems that support intelligent or autonomous capabilities. The current Trusted Foundry program provides an interim solution through the leveraging of a dual-use commercial facility, but foreign ownership and global commercial competition will reduce DoD's ability to impose restrictions on the workforce.

The Department will need to analyze this risk and define a long-term strategy that includes plans for design, fabrication, and logistics. The design phase needs to be protected from both malicious manipulation and design exfiltration, but trusted ASIC design is within DoD's ability to control at a low level of risk. Promising research results from the Defense Advanced Research Projects Agency (DARPA), the Intelligence Advanced Research Projects Activity (IARPA), and other agencies offer the potential for a technology-enabled strategy that can use widely sourced parts confidently rather than depending on a sole source Trusted Foundry. Continued research and development (R&D) is needed, and a framework is provided in Appendix A that can serve as a basis for planning further R&D investment programs.

12. U.S. Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC), "Success Stories – The MORE Tool." Available at: https://www.amrdec.army.mil/amrdec/success-more.html (Accessed November 2016.)
13. U.S. Government Accountability Office, *Counterfeit Parts: DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*, GAO-16-236 [2016]. Available at: http://www.gao.gov/products/GAO-16-236 (Accessed December 2016.)

Weapons in the field today are of special concern. They were not developed under the Program Protection Plans in place today. Also, critical components were not identified in a consistent manner and original suppliers were not subject to the vetting now required. Any existing vulnerabilities continue with no formal process for mitigation.

OVERARCHING RECOMMENDATIONS

The task force recommends that USD(AT&L) strengthen lifecycle protection policies, enterprise implementation support, and R&D programs. Such efforts will ensure that systems are designed, fielded, and sustained in a way that reduces the likelihood and consequence of cyber supply chain attacks.

In addition, the task force recommends that USD(AT&L) direct development of sustainment Program Protection Plans for critical fielded weapons systems. Military Service Chiefs should designate fielded weapons systems for development of initial sustainment PPPs to demonstrate their effectiveness.

SUMMARY

The nation's weapons systems are at risk from the malicious insertion of defects or malware into microelectronics and embedded software, and from the exploitation of latent vulnerabilities in these systems. Active search for vulnerabilities using Cyber Awakening exercises can identify and classify vulnerabilities, can enable sharing of vulnerability information, and can inform training needs. Most importantly, the effective use of expert resources will improve protection against cyber threats throughout a weapons systems lifecycle.

Appendix A: Directions for Research to Assure Supply Chain Security

APPROACHES TO ASSURANCE

Processes to enhance assurance standards for the hardware and software of DoD systems will be aided by a careful consideration of how differing approaches to trust will affect the implementation of assurance standards. Viewed abstractly, assurance can be increased in an artifact or process *"S"* by relocating what is trusted—i.e., trust in *"S"* could be made to follow from trust in something else (say) *"S'*,*"* which is more trusted than *"S."* For example, encapsulating a chip in a tamper-proof case promotes trust that the chip has not been altered only because the tamper-proof technology is trusted. The tamper-proof case increases assurance when there is concern with attacks that involves physical access to the chip before or after it has been installed. But a tamper-proof case does not defend against attacks that compromise the design or fabrication of the silicon wafer. If those are the attacks of concern, then there is little reason to have more trust in the encapsulated chip than in the original.

A collection of means will be needed to defend against the broad spectrum of possible supply chain attacks. Individual means might protect only some artifacts or processes involved in creating the microelectronics subsystem, but a collection of means could cover the subsystem for its full lifecycle: building blocks and design, then synthesis, followed by installation, maintenance, and ultimately decommissioning. The completeness of such a defense could be established by analyzing its coverage relative to the operator's understanding of what attacks are likely or feasible, and to expectations about adversary capabilities. To strengthen this analysis of coverage, a worthy research goal is to:

1. Develop formal languages for rigorously describing the scope for a means of defense given some assumed attack classes and capabilities for attackers

2. Devise algorithms to perform automated analyses that determine coverage to the provided means (and report gaps that remain)

AXIOMATIC BASIS FOR ASSURANCE

Means to establish assurance in an artifact or process will be axiomatic, analytic, synthetic, or some combination. An axiomatic basis for trust gives the weakest form of assurance. With this type of defense, an artifact or process is trusted based on beliefs that have been accepted on faith. Something might be trusted, for example, because it is sold by a given company. In this case, trust is relocated from the object to the company, thereby putting faith in the company's actions being consistent with its reputation. Here, the basis for trust has nothing to do with the artifact itself or with the manner in which it was assembled, hence why this basis for trust provides a weak form of assurance.

In the scientific literature, a small number of assertions are enshrined as axioms when they are well understood and universally accepted because they have never been contradicted by experiment. It is far less compelling to put faith in a person's nationality, a company, or any attribute that is not inherently coupled to guarantees about performance. Moreover, an axiomatic basis for trust cannot be dispositive

for any system that is too complex to understand completely—especially systems based on cutting-edge technology that have not been used in their intended environments.

ANALYTIC BASIS FOR ASSURANCE

With an analytic basis for trust, testing or reasoning are used to justify conclusions about properties of interest. Trust in an artifact or process is being relocated to trust in some method of analysis. The feasibility of establishing an analytic basis depends on the amount of work involved in performing the analysis and on the soundness of any assumptions underlying that analysis.

- Testing: In theory, every input can be checked to conclude that some given property of interest will always be satisfied, but enumeration and checking of all possible inputs is not feasible for even a simple microelectronic subsystem because, typically, only a subset of the inputs would be checked. Thus, an assumption is being made that enough inputs are being checked to expose evidence of compromise. There is also an assumption that the evaluated attributes for each test are a sufficiently complete characterization of the subsystem's behavior to ensure confidence that said tests would reveal compromises.
- Formal Verification: Designs are often amenable to mathematical analysis, either by hand or automated in software. Such analysis is tantamount to proving a theorem about some model (e.g., a program or a circuit) so that it has sufficient fidelity to detect problems without losing them in translating to an abstraction. Today's state-of-the-art for such automated analysis:

    a. Allows certain simple properties to be checked automatically for artifacts even if quite large.

    b. Allows rich classes of properties to be verified by hand for (only) small artifacts.

Research in formal verification has steadily made progress on widening the class of properties that can be checked automatically, the size and complexity that can be handled, and the fidelity of models that are analyzed. This research should be continued. It is the foundation for enhancing the capabilities of automated analysis for detecting supply chain attacks (or many other types of attacks as well).

Analytic methods are most relevant when there is a model that spans all relevant uses and all interfaces to the environment. That is, the model must not ignore too many details. Complex systems, especially microelectronic systems with cyber-active components, hardly ever admit even the theoretical possibility of such a complete model. For example, when testing or analysis is focused on some set of interfaces, the assumption is that there are not additional interfaces. This assumption can be dangerous. By ignoring power usage and electromagnetic emissions (as well as other physical properties), for instance, other avenues of information leakage could also be ignored. This means that testing or analysis might determine that classified information cannot flow to an unclassified user, even though secrets actually can leak.

SYNTHETIC BASIS FOR ASSURANCE

Finally, trust in an artifact or process can be ascertained because of its structure or how it was built. This is a synthetic basis for trust. Here, trust in the whole derives from trust in the way components that are being combined—a form of divide and conquer. For example, a synthetic basis for trust in artifact *"A"* of interest could require that:

1. The design ensures that the use of unaltered components yields an instance of *"A"* that behaves as intended.
2. Means are employed for the components to be trusted.
3. Every step in assembling, transporting, and operating *"A"* can be trusted.

Notice, (3) implies that if inputs to a step can be trusted, then the outputs from that step can be trusted as well. Also, the steps in (3) together must cover the entire lifetime of the system. So, for instance, transporting an artifact from one location to another during manufacture or even warehousing would be considered a step or part of a step.

When using a synthetic basis for trust, it pays to employ a method of composition that is linked to a procedure for establishing trust in the outputs of that method (assuming trust in the constituents). In fact, such linkages are a reason that employing a synthetic basis for relocating trust is so attractive. However, the full benefit of this synthetic trust requires that assurance be a consideration at every step of design and implementation, from the smallest components to final subsystem realization. Thus, more research is required to foster a "propagation of assurance" approach for the entire microelectronic subsystems found in today's weapons systems.

CREATING AND LEVERAGING INDEPENDENCE

Replication is an especially important synthetic basis for trust. This structure combines 2t+1 replicas, ensures all receive a copy of each input, and votes on the replica outputs. Provided the replicas are independent—that is, a supply chain attack that affects the behavior of one replica will not have the same effect on another—then the replicated system will not be compromised and will remain available until t+1 of the replicas have been compromised (which, by the independence assumption, requires t+1 different supply chain attacks). But creating this t+1-fold increase in attacker work grows the system cost over 2t+1 fold.

Independence also is leveraged in split-fabrication approaches to building systems as mentioned earlier. Here, the system is assembled from separate partitions. These partitions are defined in such a way that a change to any subset causes easily detected misbehavior by the full system. By requiring the partitions to be independent, the attacker is forced to compromise the sources of multiple partitions in order to compromise the full system. This raises the cost of supply chain attacks. Split-fabrication is, today, feasible for certain (but not all) kinds of semiconductor packagings. Theoretical results about so-called "multi-party computations" offer the possibility that similar splitting could be used for software, though additional research is needed before the protocols will be practical. Whether the basic idea can be employed at the board level or above is an open question, requiring future research.

Achieving independence is clearly quite important for defending against supply chain attacks. Blind buys, purchasing like components from separate producers, and contracting for diverse designs are all ways to develop the required independence. In addition, researchers have been investigating algorithms for creating artificial diversity. Such an algorithm, when given a single instance of a program or circuit description as input, will output a set of randomly perturbed but functionally equivalent instances. Elements of this set, by construction, perform the same task. Yet, the elements of the set will require different attacks to affect the same compromise, making these elements independent from each other with respect to supply chain attacks. Address space layout randomization (ASLR) in the Windows operating system is an example of such an algorithm. Further research should allow the Department to use the same general approach for creating independence in a broader range of systems (including FPGA descriptions and other regularly structured hardware substrates). In addition, further research can help understand the effects of combining different schemes for creating artificial diversity as well as how to compose subsystems that have been randomly perturbed in different ways.

PUTTING IT TOGETHER

Modern weapons systems have large numbers of microelectronic parts. A part may have millions of circuit elements, with complex interconnections. Also, some of the parts will be connected to sensors, and almost all of the parts will likely have thousands to millions of lines of programming (i.e., embedded firmware) that governs behavior. As a result, these microelectronic parts are too complex for comprehensive modeling. Moreover, the parts are often made by a global supply chain, with producers who may be unwilling to share design fabrication information in sufficient detail to enable analysis.

Consequently, the Department is limited primarily to axiomatic approaches for justifying trust in these lowest-level components, although sampling and extensive testing can be and are used to justify increased trust in component sources. Analytic and synthetic bases for trust remain available to manufacturers of weapons systems and to their subcontractors who are tasked with combining these lowest-level components. For example, the following collection of elements might be seen in a supply chain defense for the microelectronics assemblies found in weapons system.

4. Axiomatic basis: Purchase instances of each part from a large and diverse set of suppliers, thereby making it too costly for an adversary to perform supply chain attacks that, with a high degree of certainty, will affect all instances of a given part.
5. Synthetic basis: Employ tamper-proof packaging and unforgeable markings to prevent tampering with parts in transit.
6. Analytic basis: Record provenance (to identify who built, shipped, warehoused or otherwise handled a part or assembly) and assign trust according to judgments about the trustworthiness of those intermediaries.
7. Analytic basis: Employ sampling to collect measurements related to the operation of a system that to the user trusts, thereby establishing norms and use these norms to evaluate whether a given instance of the system can be trusted because it is equivalent to the instance measured.

Each of elements (1) through (4) could potentially be more effective were it the starting point for some research. For (1), DoD is likely to use practical judgments such as shared ownership, common subcontractors, and geo-political connections when assessing whether two suppliers are diverse. Research might reveal better evaluation criteria (e.g., company structure, current customers and suppliers, financial state) for predicting likely independence of components from different suppliers. Continued research into tamper-proof packages and markings (element (2) above) is needed because of the co-evolution of attacks and defenses. Using provenance (element (3)) as a basis for trust clearly benefits from research in support of elements (1) and (4). And there has been, and continues to be, considerable research in testing (element (4)). This framework can also be found in the approach to "design for testability" where scan-chains or other maintenance interfaces are created for loading and accessing internal state, but with the focus on detecting benign faults. Other research in testing attempts to identify counterfeits. But the Department would benefit from funding testing approaches (perhaps supported by new design regimes that stipulate certain kinds of interfaces or decomposition) to determine if the internal logic has been altered to provide added function, perhaps in response to a triggering event.

SUPPORT FOR SELF- VERSUS NON-SELF DETERMINATIONS

By definition, support for reflection entails having an interface for learning a system's state and its implementation. Reflection thus provides a way to characterize a system in terms of what it actually is, as compared to using some identifier for what the system is purported to be—i.e., "a book is not identified by its cover," but rather identified by the sequence of characters it contains. Thus, it is important to have an interface available for reflection aids in detecting a compromised component because the interface exports information that can be compared against what is expected for an un-compromised component. Notice, for detecting a successful supply chain attack, it is not actually necessary to query specific parts of the state or implementation; it suffices to receive a summary that incorporates all the state and implementation details.

A cryptographic hash H(b) of a bit string *"b"* is a relatively small value (e.g., 256 bits) that is likely to change in an unpredictable way if any of the bits in *"b"* are changed. Cryptographic hashes thus implement for software or data the summary discussed above. So given a way to compute cryptographic hashes, some data or software (including firmware) can be checked for potential gaps. Such support is available today in COTS hardware, either as part of a standard processor (e.g., Intel's® Software Guard Extensions (SGX)) or as a co-processor (e.g., the Trusted Computing Group's Trusted Platform Module (TPM)). Few embedded computing systems take advantage of that functionality, though the research community has been exploring an embodiment (known as measured principals) for deploying the approach on personal computers and cloud servers. Further research investments will be necessary, both for the more prosaic aspects of running a system—software upgrades, system back-up, and day-to-day configuration changes (i.e., setting a new target location) bring new challenges—and also for understanding deployment issues on embedded computers.

Reflection capabilities for hardware are far behind what is possible for software. Scan-chains and other maintenance interfaces do provide visibility into some aspects of a system's implementation and expected behaviors. Additional research could lead to architectures for achieving greater visibility

through these interfaces, making them effective for detecting symptoms of a supply chain attack. But because a program can always be written to simulate any given program, attackers in theory can create a compromised component that (until some trigger is activated) provides the same input and output functionality as an uncompromised component. Volkswagen's software for cheating pollution tests is an example of such a simulator.

Research advances in the following will make it harder for attackers to succeed, at least with post-deployment supply chain attacks:

- Non-digital operating attributes, such as timing, acoustic, thermal, or electromagnetic emissions, can allow a compromised component to be distinguished from a non-compromised one, even if both components seem to provide the same input and output functionality. Additional research is needed about how best to incorporate such measurements into an embedded system.
- Physically unclonable functions (PUFs) are circuits that evaluate some (unique) function that can be invoked by the chip hosting the circuit; the actual function computed depends on randomness found in hosting chip's silicon substrate. Alter the chip in any way and the functions implemented by its PUFs are likely to change. A PUF behaves like a hash function for a chip.
- Dielets present a method to verify the trustworthiness of a protected electronic component. A dielet would be inserted into the electronic component's package at the manufacturing site or affixed to existing trusted components, without altering the component's design or reliability. It could be queried at any time and would indicate if any tampering had occurred.
- Systems designed around subsystems that proactively perform periodic and automated self-testing and environment-testing are more resilient to post-deployment supply chain attacks. This is because multiple components of the subsystems would have to be altered in order to prevent the periodic testing from exposing a successful attack. Research would improve understanding of how best to build systems in this style.
- For larger assemblies, optical inspections can detect whether alterations have been made. The inside of a chip or a full circuit board could be inspected and this image could be compared with that of another image taken at an earlier time as a means to detect alterations.

Appendix B: Cyber Awakening Exercises

Contact the Defense Science Board office to access this appendix.

Appendix C: Joint Federated Assurance Center Charter

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

February 9, 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Policy Memorandum (PM) 15-001 – Joint Federated Assurance Center (JFAC) Charter

EXPIRATION DATE: February 9, 2017

POINT OF CONTACT: For more information, contact the Office of the Deputy Assistant Secretary of Defense for Systems Engineering 571-372-6129

Section 937 of the National Defense Authorization Act for Fiscal Year 2014, Public Law 113-66, requires the Department of Defense to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, acquired, maintained, and used by the Department.

Effective immediately, I am directing the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) to implement the attached Joint Federated Assurance Center (JFAC) Charter.

Attachment:
As stated

Appendix C: Joint Federated Assurance Center Charter

Joint Federated Assurance Center Charter

1. PURPOSE AND SCOPE. This charter establishes and describes the Joint Federated Assurance Center (JFAC) mission, functions, construct, and responsibilities in accordance with the Department's Acquisition and Trusted Defense Systems strategy and policy.

2. REFERENCES:

a. Public Law 113-66, National Defense Authorization Act for Fiscal Year 2014, section 937. Joint Federated Centers for Trusted Defense Systems for the Department of Defense

b. Public Law 112-239, National Defense Authorization Act for Fiscal Year 2013, section 933. Improvements in Assurance of Computer Software Procured by the Department of Defense

c. Public Law 111-383, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, section 932, Strategy on Computer Software Assurance

d. Public Law 110-417, Duncan Hunter National Defense Authorization Act for Fiscal Year 2011, section 254. Trusted Defense Systems

e. Interim Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System

f. DoDI 5200.44, Protection of Mission and Critical Functions to Achieve Trusted Systems and Networks (TSN)

g. NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

3. BACKGROUND. Interim DoDI 5000.02, Operation of the Defense Acquisition System (reference e.), and DoDI 5200.44 (reference f.) define and implement the policy and strategy for TSN within the Department for covered programs. They require program offices to include software assurance (SwA) and hardware assurance (HwA) as part of program protection planning throughout the acquisition life cycle. Program offices and sustaining activities can leverage the JFAC to support the implementation of DoD SwA and HwA requirements.

4. MISSION and OBJECTIVES. The JFAC is the federation of all Department entities having software and hardware assurance capabilities needed by programs. The JFAC will develop, maintain, and offer software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across the Military Departments, Defense Agencies, and other DoD organizations. The JFAC facilitates collaboration across Science and Technology (S&T), acquisition, Test and Evaluation (T&E), and sustainment efforts to ensure that SwA and HwA capabilities and investments are effectively planned, executed, and coordinated across the Department. The JFAC:

Appendix C: Joint Federated Assurance Center Charter

a. Supports program offices across the life cycle by identifying and facilitating access to Department SwA and HwA expertise and capabilities, policies, guidance, requirements, best practices, contracting, training, and testing support.

b. Ensures requirements to innovate software vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development.

c. Ensures requirements to innovate hardware vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development.

d. Establishes and enables efficient and affordable acquisition and use of tools for SwA and HwA analysis and test.

5. JFAC FUNCTIONS. The JFAC:

a. Identifies, promotes, and facilitates access to SwA and HwA capabilities in support of program offices, other DoD, and other Federal Government organizations throughout the acquisition life cycle, to include:

1) Efforts to ensure an inventory of SwA and HwA resources, across DoD, including vulnerability analysis tools;
2) Increasing awareness of vulnerability analysis tools, evidence-based practices, support environments, competencies, threats, and vulnerabilities; and
3) Coordinating access to and capability for applying tools, evidence-based practices, support environments, and expertise across the Department.

b. Acts as the DoD contact for interagency efforts for SwA and HwA policies, guidance, standards, acquisition practices, best practices, training, and testing support.

c. Evaluates, over time, the impact of DoD investments and activities in support of SwA and HwA.

d. Supports Department-level inquiries, studies, and reports regarding SwA and HwA.

6. JFAC MANAGEMENT CONSTRUCT:

a. The JFAC comprises the existing supporting staff and elements selected by the participating DoD Component heads, or their designees, to collaboratively carry out JFAC activities to achieve the Steering Committee's strategies and objectives. Representatives from other Federal Government agencies may be invited to participate in the JFAC.

b. The JFAC Steering Committee includes senior executive representatives from the following DoD Components:

Appendix C: Joint Federated Assurance Center Charter

1) OUSD(AT&L)
2) DoD CIO
3) Department of the Army
4) Department of the Navy
5) Department of the Air Force
6) Missile Defense Agency
7) National Security Agency
8) National Reconnaissance Office
9) Defense Information Systems Agency
10) Defense Microelectronics Activity

c. The JFAC Working Group comprises, but is not limited to, the Steering Committee policy and technical representatives with responsibility to accomplish the Steering Committee's strategies and objectives. Additional members may be approved only by the Steering Committee.

7. RESPONSIBILITIES.

a. USD(AT&L) shall:

1) Identify resource gaps, and strategies to mitigate them.
2) Preside at all meetings of the JFAC Steering Committee and associated working groups, and provide administrative management of and support for the JFAC.
3) Integrate JFAC SwA and HwA findings into DoD acquisition policy, guidance, and processes, as appropriate.
4) Assure DoD R&D strategy is informed by SW and HW assurance capability needs.

b. DoD CIO shall:

1) Invite comments from the JFAC when establishing standards and requirements for HwA and SwA to protect DoD information technology.
2) Integrate JFAC findings regarding use of Department SwA and HwA capabilities into cybersecurity policies, guidance, controls, and practices.
3) Collaborate with OUSD(AT&L) to ensure alignment between cybersecurity elements including policies, controls, guidance, and practices, and DoD acquisition elements including policy, guidance, and practices, for SwA and HwA.

c. JFAC Steering Committee shall:

1) Develop the JFAC vision, goals, and objectives, provide oversight, and maintain accountability.
2) Review and approve the JFAC concept of operations (CONOPS), as required.
3) Review JFAC capability gap analysis and approve needed modifications.

Appendix C: Joint Federated Assurance Center Charter

d. JFAC Working Group shall:

1) Develop and update the JFAC CONOPS, as required.
2) Oversee operational execution of the JFAC.
3) Use JFAC performance and metrics to determine and report return-on-investment, as required.
4) Assess JFAC capabilities and capability gaps and recommend mitigations, as required.
5) Resolve conflicting policies, schedules, and priorities.

e. JFAC supporting staff shall:

1) Execute the JFAC CONOPS, which includes performing SwA and HwA tasks and conducting capacity gap analyses.
2) Support development of and updates to the JFAC CONOPS and JFAC operation, as required.
3) Recommend and supply metrics for JFAC performance and SwA and HwA.
4) Identify and maintain cognizance of JFAC operational capabilities and capability gaps, including resources needed to address the gaps, by priority.
5) Identify and analyze reported vulnerabilities in software and hardware, including systemic patterns of causation and mitigation approaches across DoD for covered programs, and other systems as appropriate, across the life cycle.
6) Monitor effectiveness of software tools and techniques, and provide data as required.
7) Interact with program offices in accordance with each DoD Component's communication plan.

f. Participating DoD Components shall:

1) Provide SwA and HwA capabilities and resources, and support for the JFAC and management construct.
2) Assist in the formulation of JFAC operational requirements.
3) Develop R&D budget requirements in coordination with the JFAC.
4) Nominate SwA and HwA capabilities and sustain inventory.
5) Develop a communication plan to manage interactions between the JFAC support staff, members and program offices.
6) Provide SwA and HwA capabilities to DoD programs and interact with program offices in accordance with each DoD Component's communication plan.
7) Execute the JFAC CONOPS based on direction and resources.

g. DMEA shall:

1) Coordinate with the office of the Deputy Assistant Secretary of Defense (Research and Development) (DASD(RD)) on requirements for the DoD R&D strategy to improve hardware vulnerability, testing, and protection tools.

Appendix C: Joint Federated Assurance Center Charter

h. NSA shall:

1) Coordinate with the Office of the DASD(RD) on requirements for the DoD R&D strategy to improve hardware and software vulnerability detection, analysis, testing, and protection tools, and
2) Support the JFAC Working Group with SwA and HwA subject matter expertise

This charter becomes effective upon signature and remains in effect until revised or rescinded.

Robert O. Work
Deputy Secretary of Defense

9 February 2015
Date

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION, TECHNOLOGY AND LOGISTICS

NOV 1 2 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Cyber Supply Chain

The defense industrial base consists of a set of cleared contractors and known performers. Capabilities developed, produced, and sustained by the defense industrial base are derived from known and, more importantly, unknown lower tier vendors and sub-suppliers that form a global supply chain supplying providing the necessary components and subcomponents. Globalization of technology introduces multiple opportunities to insert defects and malware into components in locations outside of US Government control which can eventually find their way into a defense system or to allow disruption of critical components at disadvantageous times.

The purpose of this study is to review the DoD supply chain risk management activities, including case reviews of specific acquisition program application and the resulting outcomes. The task force will assess whether current practices are able to effectively mitigate malicious supply chain risk, and whether opportunities exist to modify or strengthen practices to increase the effectiveness of current practices. Questions the task force will address include: Are the practices resulting in actionable risk mitigations that programs have implemented to reduce system vulnerabilities? Would there be benefit to a narrowed focus on a specific supply chain risk (i.e. microelectronics)? Can DoD practices be augmented with private sector actions? What can the industrial base do to improve supply chain management practices, and what commercial sector tools and practices might be brought to bear? Finally, since this is a cross-cutting threat that affects more than DoD, are there interagency activities that DoD could better leverage to reduce its risk?

I will sponsor the study. The Honorable Page Hoeper and Dr. John Manferdelli will serve as Co-chairmen of the study. Ms. Melinda Reed, OUSD(AT&L), will serve as Executive Secretary. Lt Col Michael Harvey, USAF, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

Members of the Study

Study Chairs

Hon. Paul (Page) Hoeper	Onpoint Technologies Inc.
Dr. John Manferdelli	Google

Executive Secretary

Ms. Melinda Reed	OUSD(AT&L)

Members

Dr. Mark Epstein	Qualcomm
Hon. Paul Kaminski	Technovation, Inc.
Mr. Steve Lipner	SAFECode
Dr. David Luzzi	Northeastern University
Dr. Michael McGrath	Private Consultant
Mr. Robert Metzger	Rogers Joseph O'Donnell, PC
Mr. Andrew Oak	Johns Hopkins University Applied Physics Laboratory
Dr. Fred Schneider	Cornell University
Dr. Robert Wisnieff	IBM

Defense Science Board

Ms. Karen Saunders	Executive Director
CAPT Hugh "Mike" Flanagan	Deputy for Operations, Navy
CAPT Jeffrey Nowak	Deputy for Operations, Navy
Lt Col Victor Osweiler	Deputy for Operations, Air Force

Staff

Mr. Marcus Hawkins	Strategic Analysis, Inc.
Dr. Toni Marechaux	Strategic Analysis, Inc.
Ms. Jeray Simms	Strategic Analysis, Inc.
Ms. Melissa Smittle	Strategic Analysis, Inc.

Briefers to the Study

April 23–24, 2015

Mr. Scott Adams	SAF/AQX
Ms. Kristen Baldwin	OUSD(AT&L)
Dr. William Chappell	DARPA
Mr. Chongkin Chin	Department of Defense
Ms. Joyce Corell	ODNI
Mr. Jeffrey Green	DoD Office of General Counsel
Mr. Steve Homeyer	ODNI
Mr. Mitchell Komaroff	DoD CIO
Mr. James Kren	Defense Security Service
Mr. Jeremy Leader	SAF/AQX
Mr. Richard Naylor	Defense Security Service
Dr. Daniel Radack	Institute for Defense Analyses
Mr. William Stephens	Defense Security Service
Ms. Ann Willis	ODNI

May 28–29, 2015

Mr. Jon Boyens	NIST
Mr. Donald Davidson	DoD CIO
Dr. Lester Foster III	EWA, Inc.
LTC Christian Lewis	DIA
Mr. Emile Monette	GSA
Mr. John Pistolessi	DIA
Ms. Angela Smith	GSA
Mr. Leo Smith	ASA(ALT)
Mr. Randy Trzeciak	CMU SEI
Mr. Thomas Tyndall	DIA
Mr. Elijah Varga	Army PEO for Missiles and Space

June 11–12, 2015

Mr. Brandon Ahrens	Ernst & Young LLP
Mr. Paul Donato	Ernst & Young LLP
Mr. Phillip Harlow	XTAR LLC
Mr. John Hauser	Ernst & Young LLP
Ms. Doree Keating	Ernst & Young LLP
Mr. Alfred Lewis Jr.	Boeing
Mr. Victor Manzueta	Joint Staff (J6)
Lt Col John Smail	Joint Staff (J6)
Mr. Andras Robert Szakal	IBM
Mr. Vijay Takanti	EXOSTAR

Briefers to the Study

July 30–31, 2015

Ms. Karen Abell	U.S. Navy Naval Air Systems Command
Ms. Kristen Baldwin	OUSD(AT&L)
Mr. Arthur Beauchamp	Defense Logistics Agency
Mr. Ron Fodor	Leidos, Inc.
Mr. Brent Gerity	Leidos, Inc.
Mr. Ted Glum	Defense Microelectronics Activity
Mr. James Gosler	The Johns Hopkins University Applied Physics Laboratory
Ms. Doreen Harwood	Leidos, Inc.
Dr. James Hayward	Applied DNA Sciences
Ms. Missy Hebb	U.S. Navy Naval Air Systems Command
Ms. Janice Meraglia	Applied DNA Sciences
Mr. Roy Wilson	U.S. Navy Naval Air Systems Command
Mr. Raymond Shanahan	OUSD(AT&L)

August 13–14, 2015

Ms. Edna Conway	Cisco Systems, Inc.
Ms. Danielle Curcio	Raytheon Company
Mr. Geoff Donatelli	Raytheon Company
Ms. Holly Dunlap	Raytheon Company
Ms. Ellen Lux	Raytheon Company
Mr. Theodore Shpak	Raytheon Company
Mr. Michael Smith	Raytheon Company
Dr. James Wade	Raytheon Company

September 17–18, 2015

Mr. Keith Bergevin	Defense Microelectronics Activity
Mr. David Brown	Intel Corporation
Dr. Ed Cole	Sandia National Laboratories
Mr. John Day	IBM
Mr. George Duchak	DIUx
Mr. Alex Gantman	Qualcomm
Mr. Ted Glum	Defense Microelectronics Activity
Mr. Steve McNeil	Xilinx Corporation
Mr. Ron Minnich	Google
Mr. Jason Moore	Xilinx Corporation
Mr. Enrique Oti	DIUx

October 29–30, 2015

Dr. Carlos Aquayo-Gonzalez	PFP Cybersecurity
Mr. Thurston Brooks	PFP Cybersecurity
Dr. Boyd Livingston	NSA

Briefers to the Study

Dr. Ian Levy	United Kingdom GCHQ
Mr. Richard Naylor	Defense Security Service
Mr. Stanley Sims	Defense Security Service
Mr. William Stephens	Defense Security Service

February 4–5, 2016

Ms. Kristen Baldwin	OUSD(AT&L)
Mr. Kerry Bernstein	DARPA
Mr. Robert Gold	OUSD(AT&L)
Mr. Brian Hughes	OUSD(AT&L)
Ms. Trisha Thibodaux	OUSD(AT&L)
Mr. Christian Thomasson	U.S. Air Force

April 18–19, 2016

COL Matthew Dunlop	U.S. Army Cyber Command
Mr. Larry Jennings	ASA(ALT)